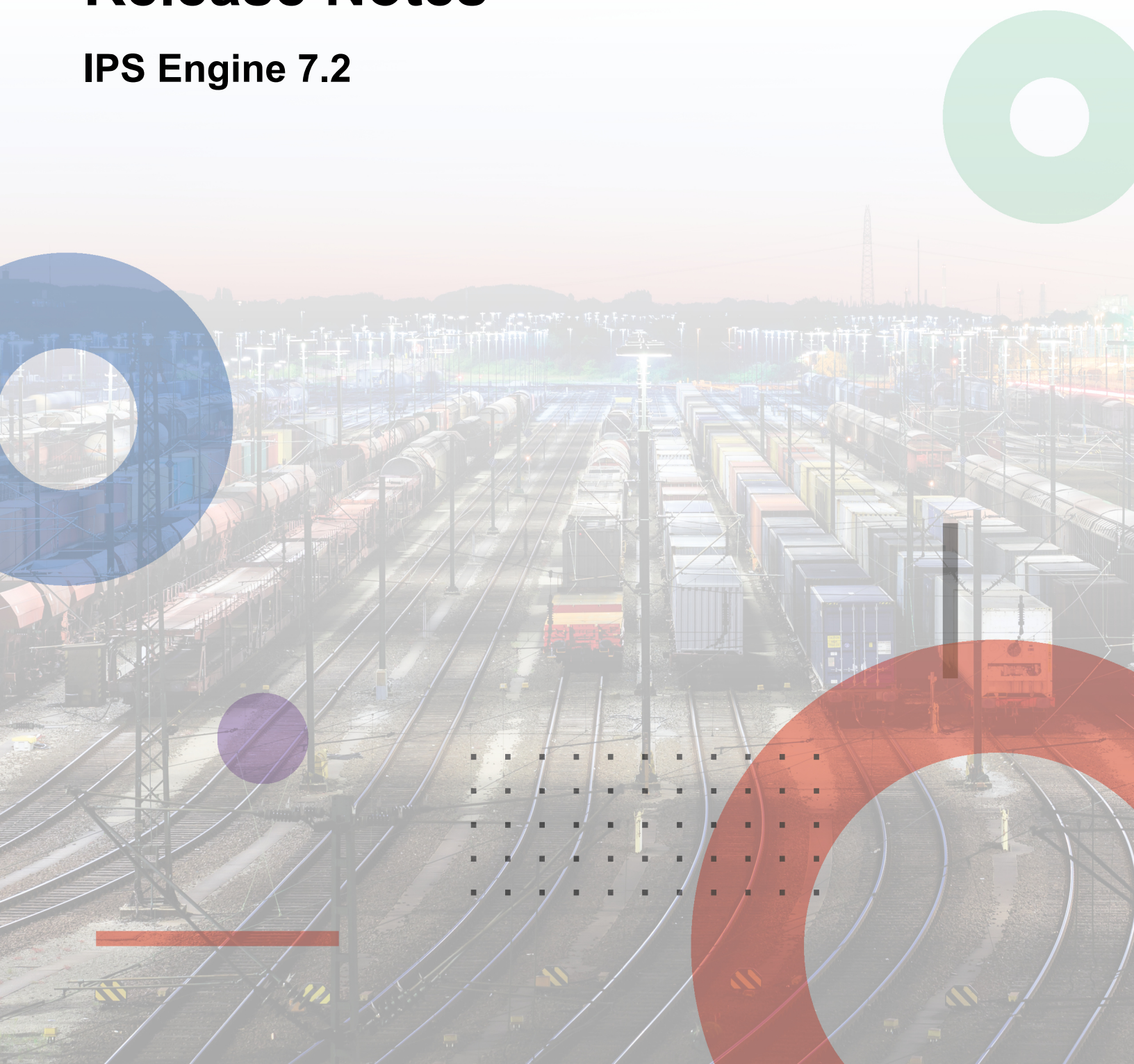
FORTINET

Release Notes

IPS Engine 7.2



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 01, 2023
IPS Engine 7.2 Release Notes
43-720-878903-20230201

TABLE OF CONTENTS

Change log

Date	Change Description
2023-02-01	Initial release.

Introduction

This document provides the following information for the Fortinet IPS Engine 7.2 build 255 (7.00255).

IPS Engine 7.2 build 255 is a release to FortiGuard. It is not a built-in release for FortiOS.

For additional FortiOS documentation, see the Fortinet Document Library.

Product integration and support

The following table lists IPS engine product integration and support information:

FortiOS	7.2

Resolved issues

The resolved issues listed do not list every bug that has been corrected with this release. For inquiries about a particular bug, contact Customer Service & Support.

Bug ID	Description
590623	FortiGate 76E has strange padding in certificate after deep inspection (ICAgICAg..).
673117	Trivial file transfer protocol (TFTP) traffic does not work well when TFTP application is set in security policy.
687885	Inconsistent system performance with RFC2544 IXIA breaking point testing.
695464	High IPS engine CPU utilization.
698247	Flow mode Web Filter override crashes and socket leaks in IPS engine daemon.
757322	Inconsistent system performance with RFC2544 IXIA Breaking point testing using frame size 68 and SR-IOV interface.
773711	HTTPS sessions to some internal destinations drop for some users from the same set of group.
774826	IPS processes consume high CPU usage.
775566	Websites do not load in flow mode with deep SSL inspection.
781110	Packets are lost with security (UTM) profiles and third party WAN optimizer (Riverbed).
786479	Traffic log does not work under next generation firewall (NGFW) mode while a reboot can solve the issue on FortiGate 101E.
787151	FortiGate inserts epoch time into the PCAP when detected by some signatures.
789861	Globus file transfer traffic breaks when Web Filter profile is enabled along with certificate inspection.
791175	Unable to access specific website after upgrading IPS Engine version.
792312	HTTPS traffic cannot pass FortiGate-VM on VMware ESXi well when IPS engine and deep inspection are enabled.
794872	FortiGate 5001E blade application IPS Engine crashes during traffic testing.
795677	Upgrading IPS Engine slows web access.
797229	TCP Middlebox Reflexion.
798367	IPS Engine treats FLOW-DLP- CIFS ZIP file block unexpectedly.
798587	NGFW security policy misses `internet-service6/internet-service6-src` options.
798817	IPS Engine crashes at `ips_dac_get_save_log` on FortiGate 401E during stress testing.
798829	IPS Engine has signal 7 crash at `ips_shm_sig_get` on firewall.

Bug ID	Description
800524	IPS engine crashes with signal 11.
800730	When using NGFW policy-based mode, modifying a security policy resets all sessions.
800731	In flow mode, antivirus sends HTML files to FortiGate Cloud Sandbox every time.
802465	ERR_SSL_PROTOCOL_ERROR occurs when loading a website in flow mode.
802683	IPS engine debug filter does not work.
804500	Changes to the custom URL filter cause a network degredation that impacts customers.
806083	DNS local domain filter does not work in flow mode.
808961	IPS engine stalls and causes packet drops.
810105	Signal 14 alarm clock received by updated and hasync crash.
811213	IPS engine with CP enabled causes high CPU usage.
811551	Traffic drops in NGFW mode after upgrade.
816032	Security policy with FSSO authentication does not match sporadically.
816759	IPS Engine crashes on `ovrd_ssl_read` on 5.00272.
817902	IPS engine crashes with signal 11.
819224	Regular expression engine is not migrated to PCRE2.
822573	URL filter cannot blocked URLs if IPS Engine sensor is on the same firewall policy with flow inspection mode.
827253	With IPv6 URL filter, FortiOS only blocks traffic to pure IPv6 and does not detect traffic to obfuscated IPv6.
834056	After upgrade, high memory consumption and several conserve modes are observed.
836955	Primary and secondary nodes of HA cluster are inaccessible and drop traffic.
839679	IPS Engine crashes with Signal 11.
840232	Hostname in syslog is short.
841269	With SSL inspection certificate, there is no block page when Application Control and Web Filter are enabled on the same policy.
848368	IPS Engine causes high memory usage.
849030	libips.so crashes with signal 11 in `sock_read_stop` on FortiOS.
854254	IPS Engine does not support sending IPv6 reset packet in IPIP tunnel.
855301	IPS engine consumes high memory.
856616	IPS engine increases memory utilization.
859675	FortiOS does not drop traffic from untrusted external IP addresses and instead presents the server certificate.

Bug ID	Description
863074	The Web Filter override function sends out block and passthrough logs.
872062	Flow-based DNS filter with safe search enabled returns A record 0.0.0.0 for redirected FQDNs on IPS Engine.

Known issues

There are no known issues with this release of IPS engine version 7.2 for FortiOS.

To report a bug, please contact Customer Service & Support.

www.fortinet.com